

Subject: GUIDANCE FOR COMMANDERS ON
PUBLICLY ACCESSIBLE WEBSITES

IMMEDIATE

O 302155Z JUN 99

FM DA WASHINGTON DC//SAIS-SACC//

TO ALARACT

UNCLAS ALARACT 061/99

SUBJECT: GUIDANCE FOR COMMANDERS ON PUBLICLY ACCESSIBLE
WEBSITES ANDNIPRNET CONNECTIVITY

1. THIS MESSAGE REITERATES GUIDANCE FROM THE CHIEF OF STAFF, ARMY ON ACTIONS COMMANDERS SHOULD TAKE TO REDUCE POTENTIAL SECURITY RISKS ON THE NIPRNET AND THEIR ORGANIZATION'S "PUBLICLY ACCESSIBLE WEBSITES" (DEFINED BELOW). COMMANDERS MUST ENSURE THAT:
 - A. ALL SENSITIVE INFORMATION (DEFINED BELOW) IS REMOVED FROM PUBLICLY ACCESSIBLE WEBSITES.
 - B. SECURITY PROCEDURES ARE IN PLACE TO MINIMIZE RISKS OF REVEALING SENSITIVE INFORMATION.
 - C. BACKDOOR CONNECTIONS FROM THE NIPRNET TO THE INTERNET (WORLD WIDEB) ARE CLOSED.
2. THIS MESSAGE APPLIES TO ALL ARMY ORGANIZATIONS THAT MAINTAIN PUBLICLY ACCESSIBLE ARMY WORLD WIDE WEB (WWW) WEBSITES AND/OR NIPRNETCONNECTIVITY. A PUBLICLY ACCESSIBLE WEBSITE IS A WEBSITE THAT HAS INTERNET ACCESS WITHOUT CONTROLLED ACCESS, SUCH AS A USERID AND PASSWORD, OR DOES NOT RESIDE ON A RESTRICTED INTRANET. IN CASES WHEREA WEBSITE'S STATUS IS UNCERTAIN, COMMANDERS SHOULD ASSUME

THAT THE WEBSITE IS PUBLICLY ACCESSIBLE. IF A WEBSITE IS CONSIDERED RESTRICTED, THIS SHOULD BE VERIFIED TO ENSURE THAT PUBLIC ACCESS IS NOT POSSIBLE.

3. ARMY WEBSITES EXIST AT ALL ECHELONS OF THE FORCE. THIS MESSAGE APPLIES TO ALL WEBSITES OPERATED BY ARMY ORGANIZATIONS REGARDLESS OF LOCATION OR ECHELON (E.G., MACOM, INSTALLATION, BATTALION ETC.).

4. ALL ARMY ACTIVITIES MUST IMMEDIATELY REVIEW ALL INFORMATION ON THE PUBLICLY ACCESSIBLE WEBSITES UNDER THEIR CONTROL. AN ARMY WEB OPERATIONS SECURITY CHECKLIST ([HTTP://WWW.ARMY.MIL/WEBMASTERS/CHECKLIST.HTM](http://www.army.mil/webmasters/checklist.htm)) HAS BEEN COMPILED TO ASSIST ARMY ACTIVITIES IN REVIEWING PUBLICLY ACCESSIBLE WEBSITE CONTENT. ANY OF THE FOLLOWING TYPES OF INFORMATION MUST BE REMOVED FROM THE WEBSITE AND MAY NO LONGER BE DISPLAYED ON PUBLICLY ACCESSIBLE WEBSITES:

A. PLANS OR LESSONS LEARNED WHICH WOULD REVEAL SENSITIVE MILITARY OPERATIONS, EXERCISES OR VULNERABILITIES,
B. REFERENCES TO ANY INFORMATION THAT WOULD REVEAL SENSITIVE MOVEMENTS OF MILITARY ASSETS OR THE LOCATION OF UNITS, INSTALLATIONS, OR PERSONNEL WHERE UNCERTAINTY REGARDING LOCATION IS AN ELEMENT OF THE SECURITY OF A MILITARY PLAN OR PROGRAM,
C. PERSONAL INFORMATION ABOUT U.S. CITIZENS, DEPARTMENT OF DEFENSE (DOD) EMPLOYEES AND MILITARY PERSONNEL INCLUDING:
(1) SOCIAL SECURITYACCOUNT NUMBERS, (2) DATES OF BIRTH, (3) HOME ADDRESSES, (4) TELEPHONE NUMBERS OTHER THAN NUMBERS OF DUTY OFFICES WHICH ARE APPROPRIATELY MADE AVAILABLE TO THE GENERAL PUBLIC, AND (5) NAMES, LOCATIONS, AND ANY OTHER IDENTIFYING INFORMATION ABOUT FAMILY MEMBERSOF DOD EMPLOYEES AND MILITARY PERSONNEL.

5. COMMANDERS ARE ENCOURAGED TO MIGRATE THEIR PUBLICLY ACCESSIBLE INFORMATION TO A SECURE, ACCESS CONTROLLED INTERNET SITE. COMMANDERS ARE URGED TO USE THE ARMY KNOWLEDGE ONLINE (AKO) INTRANET SITE, AND SHOULD CONTACT THE ARMY AKO HELP DESK BY EMAIL (AKOHELP@US.ARMY.MIL) FOR MORE INFORMATION.

6. AS A TOP PRIORITY, COMMANDERS SHOULD EXAMINE ALL CONNECTION TO THE NIPRNET TO ENSURE THAT THERE ARE NO "BACKDOORS" THAT WOULD PERMIT UNPROTECTED ACCESS FROM THE INTERNET TO ARMY SYSTEMS CONNECTED TO THE NIPRNET.

7. THIS GUIDANCE FROM THE ARMY CHIEF OF STAFF IS BEING RESTATED BECAUSE COMPUTER ATTACKS AND PENETRATIONS HAVE

RISEN SUBSTANTIALLY. THIS IS A FORCE PROTECTION ISSUE. OUR
INTENT IS TO BALANCE THE ARMY'S SECURITY NEEDS WITH OUR
REQUIREMENT TO RELEASE APPROPRIATE INFORMATION TO THE
PUBLIC AND TO LEVERAGE THE ADVANTAGES OF INTERNET
TECHNOLOGY. ADDITIONAL GUIDANCE ON PROTECTION OF THE
NIPRNET, TO INCLUDE POLICIES ON IMPLEMENTATION OF PUBLIC
KEY INFRASTRUCTURE (PKI), WILL BE PUBLISHED IN THE NEAR
FUTURE. QUESTIONS ABOUT THIS MESSAGE SHOULD BE SENT VIA
EMAIL TO THE ARMY WEBMASTER (WEBMASTER@US.ARMY.MIL).
EXPIRATION DATE CANNOT BE DETERMINED

BT

NNNN